

信息与软件工程学院上机实验报告

(第 4 次)

一、实验名称

实验四：网络信息扫描实验

二、实验目的及要求

通过练习使用网络端口扫描器，可以了解目标主机开放的端口和服务程序，从而获取系统的有用信息，发现网络系统的安全漏洞。在实验中，练习使用 SuperScan 网络端口扫描工具。通过端口扫描实验，增强网络安全方面的防护意识。

通过使用综合扫描及安全评估工具，学习如何发现计算机系统的安全漏洞，并对漏洞进行简单分析，加深对各种网络和系统漏洞的理解。在实验中，练习使用流光 Fluxay5 和 SSS。

三、实验环境

1. 实验平台：VMware Workstation Pro 25H2
2. 操作系统：两台 Windows 7 64-bit SP1 虚拟机，分别命名为 VM-A 和 VM-B
3. 网络环境：同一局域网，扫描地址段为 192.168.59.0/24，其中 VM-A 的 IP 地址为 192.168.59.131，VM-B 的 IP 地址为 192.168.59.129
4. 扫描工具：SuperScan 3.00、流光 Fluxay5、Shadow Security Scanner (SSS)

四、实验设计

1. 实验步骤

实验环境在同一台主机中部署了两台 Windows 7 虚拟机，并将两台虚拟机接入同一局域网。扫描工具安装在其中一台虚拟机中，作为发起扫描的主机；另一台虚拟机作为被扫描主机参与实验。实验开始时先通过 Ping 扫描确认网段中

的活动主机，再对活动主机进行端口扫描，随后使用流光和 SSS 分别对扫描结果进行补充和验证。

2. 调试过程及实验结果

2.1 使用 SuperScan 扫描

(1) Ping 功能

打开 SuperScan 后，在 IP 范围中输入起始地址 192.168.59.1 和终止地址 192.168.59.255，在扫描类型中选择“仅仅 Ping 计算机”，然后启动扫描。扫描结束后，结果窗口显示该网段内共有两台活动主机，分别为 192.168.59.129 和 192.168.59.131。

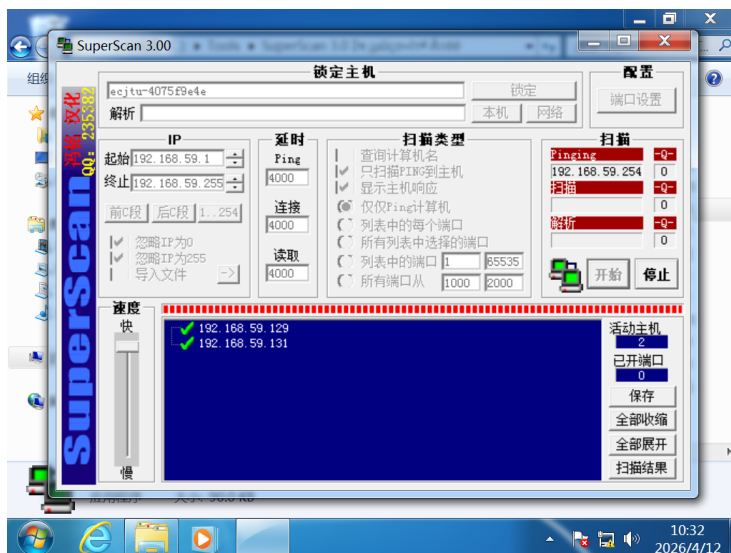


图 1: SuperScan Ping 扫描结果

Ping 扫描结果给出了活动主机数量和主机列表，后续端口扫描即可在这些在线主机的基础上继续进行。

(2) 端口扫描功能

在端口扫描前，先进入端口配置界面，对扫描端口列表进行查看和选择。截图中使用的是保存好的端口列表文件，界面中可以看到多个常见端口已经被加入扫描列表。



图 2: SuperScan 端口配置界面

端口列表设置完成后，返回主界面，选择“列表中的每个端口”进行扫描，并展开扫描结果。扫描窗口显示共有两台活动主机、共发现 6 个开放端口。从展开结果可以看到，192.168.59.129 和 192.168.59.131 均检测到 135、139、445 端口开放，其中对应服务分别为 DCE endpoint resolution、NETBIOS Session Service 和 Microsoft-DS。

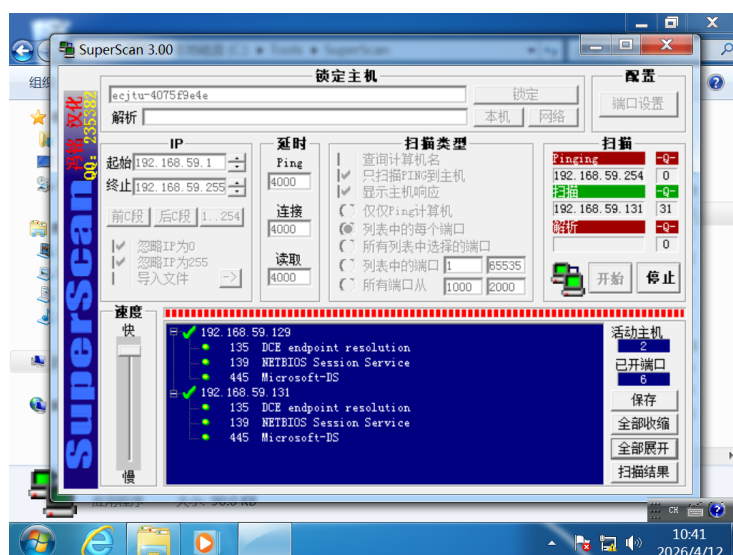


图 3: SuperScan 端口扫描结果

扫描结果显示，目标网段中的两台活动主机都开放了与 RPC、NetBIOS 和文件共享相关的端口，后续可以据此继续进行综合扫描和服务识别。

2.2 流光 Fluxay5 的使用

(1) 综合扫描结果

启动流光后，打开“高级扫描向导”，依次设置起始地址和结束地址，勾选 Ping 检查以及 PORTS、FTP、TELNET、IPC、IIS、PLUGINS 等检测选项，并将端口扫描方式设置为“标准端口扫描”。其余 POP3、FTP、SMTP、IMAP、Telnet、CGI、SQL、IIS、MISC 和 PLUGINS 相关设置保持默认，最后指定报告保存位置并开始扫描。探测结果窗口记录了对 192.168.59.129 和 192.168.59.131 的扫描结果，可以看到两台主机的 IPC 空连接建立成功，同时检测到 192.168.59.129 的 139 端口和两台主机的 445 端口开放。



图 4: 流光 Fluxay5 探测结果

扫描报告进一步按主机记录了服务识别结果。截图中可以看到，192.168.59.131 标识为 VM-A.localdomain，检测到 445 (Windows 2000 SMB)；192.168.59.129 标识为 VM-B，检测到 445 (Windows 2000 SMB) 和 139 (SMB)。结合探测结果窗口，可以把主机地址、主机名、开放端口和对应服务对应起来。



图 5: 流光 Fluxay5 扫描报告

流光的扫描结果补充了主机名和服务类型信息，使扫描结果比单纯的端口列表更完整。

2.3 使用 SSS 漏洞扫描

(1) Quick Scan 扫描结果

打开 SSS 后，使用 Quick Scan 对 192.168.59.129 进行扫描。扫描结果界面显示目标主机名为 VM-B，右侧给出了主机的基本信息、扫描起止时间以及 TCP 端口信息。结果中列出了 135、139、445 三个端口，其中对应的服务分别为 RPC-LOCATOR、NETBIOS-SSN 和 MICROSOFT-DS。

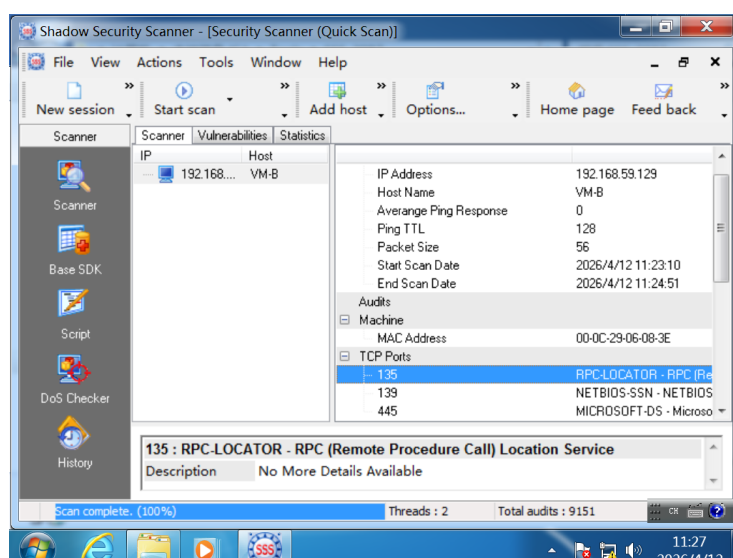


图 6: SSS Quick Scan 扫描结果

SSS 的扫描结果与前面 SuperScan 和流光得到的主要端口信息基本一致，说明不同扫描工具对目标主机开放服务的识别结果具有对应关系。

3. 总结

3.1 对上机实践结果进行分析

本次实验依次完成了 Ping 扫描、端口扫描、综合扫描和漏洞扫描三个部分。SuperScan 先给出了局域网中的活动主机列表，再给出目标主机开放端口；流光在端口结果基础上补充了 IPC、主机名和服务识别信息；SSS 则进一步用 Quick Scan 的方式验证了目标主机的开放端口情况。三个工具得到的主要端口结果之间具有对应关系，其中 135、139、445 是实验中反复出现的主要端口。

从实验结果来看，扫描过程已经能够完成从主机发现到端口识别，再到服务和扫描报告生成的完整链路。通过这些结果，可以较清楚地看到目标主机在局域网中的在线状态、开放端口以及相关服务信息，这些信息也是后续进行网络安全分析和主机安全加固时的重要依据。

3.2 上机的心得体会

本次上机把主机发现、端口识别、服务识别和安全扫描串联起来进行了一次完整验证。实际操作中可以看到，不同扫描工具的侧重点并不完全相同：SuperScan 用于快速发现主机和端口，流光用于补充主机名、端口和服务识别信息，SSS 用于对单台主机进行进一步扫描。将几种工具的结果进行对照后，端口扫描、服务识别和综合安全扫描之间的关系更加清晰。

3.3 改进意见

后续可进一步细化目标范围设置，例如只针对单台主机或固定端口范围进行扫描；也可以把不同扫描工具的结果整理成统一对照表，便于比较端口识别和服务识别的一致性。如果实验环境允许，还可以结合抓包工具观察扫描过程中的网络数据包，进一步分析不同扫描方式对应的报文特征。